sysdig SECURE EVERY SECOND.

2025 Cloud-Native Security and Usage Report

Executive Summary

The "Sysdig 2025 Cloud-Native Security and Usage Report" is back for its eighth year, analyzing real-world data and the current state of cloud security and container usage. The findings detailed here indicate that security teams have made significant advancements across key areas, not only year over year, but also looking back on previous reports. With this in mind, our 2025 report provides benchmarks for maturity and efficiency, helping security teams, developers, and organizational leaders measure progress in the coming year.

In October 2023, the Sysdig Threat Research Team (TRT) concluded that cloud attacks can take place in 10 minutes or less. In this report, we have detailed how organizations today are detecting, investigating, and responding to real-world threats within this time frame using innovative tools and techniques. We've also found that open source software is not just a trend, but has become a dependency for today's cloud security. The open source threat detection tool Falco has been downloaded over 140 million times and is used across large enterprises and small businesses (SMBs) alike, signaling that organizations of all sizes have found value in the power of open source security.

The security community has also made advancements in vulnerability management and AI workload security. For the second year in a row, we've identified a significant reduction in runtime vulnerabilities. We also saw significant growth in the number of workloads that use AI and machine learning (ML) packages and — despite this growth — the percentage of workloads publicly exposed to the internet has decreased significantly, an indication that organizations are prioritizing AI security.

In assessing identity management from a different perspective than years past, we found that organizations are managing exponentially more service accounts than user accounts, and that these service accounts present higher risk profiles. No wonder supply-chain attacks have become increasingly common!

Finally, in a few surprising turns of events, it turns out that organizations are prioritizing nuanced technical security benchmarks for compliance policies over the federally prescribed regulations we often read about in the news. And last but certainly not least, our beloved container lifespan statistic of many years has taken a new form. Short-lived workloads are purpose-built for speed and only live long enough to complete their task — all the more reason for real-time detection and continuous monitoring.

Read the full report for all of this year's findings.

DOWNLOAD THE REPORT →

Key trends

Machine identities are 7.5x more risky than human identities and there are up to 40,000x more of them to manage

Workloads using AI/ML packages grew by 500% and public exposure decreased by 38% over the last year, showing that secure AI implementation has become a clear organizational priority

Real-time detection and response in under 10 minutes — when tools alert within seconds — is possible, and companies are initiating response actions in under 4 minutes

60% of containers live for 1 minute or less

In-use vulnerabilities have decreased to less than 6%, but image bloat quintupled year over year

Organizations across the globe in all business sectors are **leveraging open source software**, like Falco, regardless of their size

Cybersecurity regulations are essential, and EU-based organizations are leading the charge by prioritizing compliance more than their global counterparts.

COPYRIGHT © 2025 SYSDIG, INC.
ALL RIGHTS RESERVED.

DOWNLOAD THE REPORT →